IN THE SPECIFICATION

Please amend the paragraph beginning at page 1, line 13, as follows:

Even more precisely, the process relates to the set of processes called "zero-knowledge Protocols", i.e. without any communication of knowledge. According to this kind of process, the authentication is carried out following a protocol that, as it is ~~recognised~~recognized, and under assumptions considers as perfectly reasonable by the scientific community, discloses nothing about the secret key of the prover.

Please amend the paragraph beginning at page 2, line 23, as follows:

The GUILLOU-QUISQUATER protocol, described in the article by L.C. GUILLOU and J.J. QUISQUATER, entitled "A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory," published in "Advances in Cryptology: Proceedings of EUROCRYPT '88; Lecture notes in Computer Sciences, vol. 330, Springer-Verlag, Berlin, 1988, pp. 123-128,

Please amend the paragraph beginning at page 5, line 8, as follows:

Though the French patent application FR-A-2 752 122 describes an ~~optimisation~~optimization of these protocols, it is restricted to protocols involving the discrete logarithm method following a mode called "with pre-calculations" that has the drawback of implying regularly scheduled reloads.

Please amend the paragraph beginning at page 11, line 8, as follows:

From the Bezout theorem, it is known that two integers exists, such as ~~ab~~ ap+bq=1

To calculate $y=x^e \pmod n$, we start by reducing x modulo each prime factor by calculating $x_p=x \pmod p$ and $x_q=x \pmod q$. We also reduce e modulo (p-1) and (q-1) by calculating e_p=e modulo (p-1) and e_q=e (modulo q-1) (in the protocol of Quillou-Quisquater, e is always lower than e-1 and q-1, then $e_p=e_q=e$ ~~$e_p=e_q=1$~~.